

A fast Fourier transform method for computing the weight enumerator polynomial and trigonometric degree of lattice rules

Josef Dick*

July 24, 2012

The weight enumerator polynomial $W_{(g_1, \dots, g_s)}$, which has previously been studied in coding theory [4, 8, 9, 12], association schemes [6], orthogonal arrays [11], spherical t -designs [1] and digital nets [3, 4, 11], of a lattice rule [7, 10]

$$\frac{1}{N} \sum_{n=0}^{N-1} f \left(\left\{ \frac{n(g_1, \dots, g_s)}{N} \right\} \right),$$

where $\{x\}$ denotes the fractional part of a nonnegative real x , $N > 1$ is an integer, and $g_i \in \{1, 2, \dots, N-1\}$, defined by

$$W_{(g_1, \dots, g_s)}(z) := \sum_{a=0}^{ds} z^a M_{(g_1, \dots, g_s)}(a),$$

with

$$M_{(g_1, \dots, g_s)}(a) := \#\{(k_1, \dots, k_s) \in \{-d, -d+1, \dots, d\}^s : k_1 g_1 + \dots + k_s g_s \equiv 0 \pmod{N}, |k_1| + \dots + |k_s| = a\},$$

can be written as

$$\begin{aligned} W_{(g_1, \dots, g_s)}(z) &= \sum_{\substack{(k_1, \dots, k_s) \in \{-d, \dots, d\}^s \\ k_1 g_1 + \dots + k_s g_s \equiv 0 \pmod{N}}} z^{|k_1| + \dots + |k_s|} \\ &= \sum_{(k_1, \dots, k_s) \in \{-d, \dots, d\}^s} z^{|k_1| + \dots + |k_s|} \frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i n (k_1 g_1 + \dots + k_s g_s) / N} \\ &= \frac{1}{N} \sum_{n=0}^{N-1} \prod_{j=1}^s \sum_{k_j=-d}^d z^{|k_j|} e^{2\pi i n k_j g_j / N}, \end{aligned}$$

where the last expression can be used to compute $W_{(g_1, \dots, g_s)}$ in $\mathcal{O}(Nds^2)$ operations, which can be reduced to $\mathcal{O}(Nds)$ operations if one wants to compute the trigonometric degree ρ [2, 5] of a lattice rule via the equality

$$\rho = \begin{cases} 0 & \text{if } M_1 \neq 0, \\ \max\{a : 1 \leq a \leq d, M_1 = \dots = M_a = 0\} & \text{otherwise,} \end{cases}$$

*School of Mathematics and Statistics, UNSW, Sydney, Australia; email: josef.dick@unsw.edu.au; The author is supported by a Queen Elizabeth 2 Fellowship of the Australian Research Council.

where the trigonometric degree is defined by

$$\frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i n(k_1 g_1 + \dots + k_s g_s)/N} = \int_0^1 \dots \int_0^1 e^{2\pi i(k_1 x_1 + \dots + k_s x_s)} dx_1 \dots dx_s = 0,$$

for all $(k_1, \dots, k_s) \in \mathbb{Z}^s \setminus \{(0, \dots, 0)\}$ with $|k_1| + \dots + |k_s| \leq \rho$, since this is equivalent to the maximum over all ρ such that

$$k_1 g_1 + \dots + k_s g_s \not\equiv 0 \pmod{N} \quad \text{for all } (k_1, \dots, k_s) \in \mathbb{Z} \setminus \{(0, \dots, 0)\} \text{ and } |k_1| + \dots + |k_s| \leq \rho.$$

References

- [1] E. Bannai, On the weight distribution of spherical t-designs. *European J. Combin.*, 1, 19–26, 1980.
- [2] R. Cools and J. N. Lyness, Three- and four-dimensional K-optimal lattice rules of moderate trigonometric degree. *Math. Comp.*, 70, 1549–1567, 2001.
- [3] J. Dick and M. Matsumoto, On the fast computation of the weight enumerator polynomial and the t value of digital nets over finite abelian groups. In preparation.
- [4] S. T. Dougherty and M. M. Skriganov, MacWilliams duality and the Rosenbloom-Tsfasman metric. *Mosc. Math. J.*, 2(1), 81–97, 199, 2002.
- [5] J. N. Lyness and T. Sørenvik, Five-dimensional K-optimal lattice rules. *Math. Comp.*, 75, 1467–1480, 2006.
- [6] W. J. Martin and D. R. Stinson, Association schemes for ordered orthogonal arrays and (T, M, S) -nets. *Can. J. Math.*, 51, 326–346, 1999.
- [7] H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*. CBMS-NSF Regional Conference Series in Applied Mathematics, 63. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.
- [8] I. Siap, The complete weight enumerator for codes over $\mathcal{M}_{n,s}(\mathbb{F}_q)$. In: *Cryptography and Coding*, Lecture Notes in Computer Science, vol. 2260, pp. 20–26. Springer, Berlin (2001).
- [9] V. M. Sidel’nikov, The spectrum of weights of binary Bose-Chaudhuri-Hocquenghem codes. *Problemy Peredači Informacii*, 7, 14–22, 1971.
- [10] I. H. Sloan and S. Joe, *Lattice methods for multiple integration*. Oxford University Press, Oxford, 1994.
- [11] H. Trinker, A simple derivation of the MacWilliams identity for linear ordered codes and orthogonal arrays. *Des. Codes Cryptogr.*, 50, 229–234, 2009.
- [12] J. H. van Lint, *Introduction to Coding Theory*. Graduate Texts in Mathematics, vol. 86, 2nd edn. Springer-Verlag, Berlin (1992).